Trade-off between End-to-End Reliable and Cost-Effective TDMA/WDM Passive Optical Networks

Abhishek Dixit, Bart Lannoo, Didier Colle, Mario Pickavet, Piet Demeester
Department of Information Technology
Ghent University-IBBT, Ghent, Belgium
abhishek.dixit@intec.ugent.be

***Abstract*— Hybrid TDMA/WDM (TWDM) Passive Optical Network (PON) is a promising candidate for Next-Generation PON (NG-PON) solutions. We propose end-to end reliable architectures for business users and a cost-effective network for residential users. We evaluate the proposed reliable architectures in terms of protection coverage, connection availability, impact of failure (i.e. to avoid a huge number of end users being affected by any single failure) and cost in different populated scenarios.**

Keywords- Resilience; Availability; Failure Impact Robustness; Hybrid TDMA/WDM PON

I. INTRODUCTION

Passive optical networks (PONs) have been widely considered as a preferred technology to implement various Fiber to the X (or FTTX, where X can mean the home, curb, cabinet, or building) solutions to deliver high bandwidth to the users at low cost and energy per bit. Many telecommunication operators have started deploying PONs to replace traditional xDSL and cable modem technologies. There has been an extensive research to further upgrade the PON technology, to meet the ever-increasing requirements of the end users in the cost and energy efficient way [1]. It is anticipated that the next-generation PON (NG-PON) - with a much higher bandwidth, a high customer fan out, long reach and flexibility in resource allocation - is a natural path forward. Hybrid time-division multiple access and wavelength division multiplexing (TWDM) PON is an actively considered NG-PON solution. Compared with other NG-PON architectures, TWDM-PON offers a relatively large splitting ratio, and consequently can achieve a lower cost and power consumption per user [2]. Moreover, it inherently supports high flexibility of resource allocation [3], which allows it to efficiently adapt to the varied traffic demands from the end user.

On the other hand, long fiber lengths with a higher fiber-cut probability, large customer hit outs, and use of active components like reach extenders (REs) with shorter failing intervals, necessitate the protection mechanisms in NG-PON. However, the level of protection required depends upon the user's profile. The businesses are run over fully protected networks and business users will like to have full protection coverage. Although the ratio of business customers to residential customers is small, the ratio of business revenue to residential revenue is about the same [4], and thus protection of business users is important for the network provider. However, the cost incurred in providing protection can in fact be considerable. Protection involves duplicating facilities like optical fiber paths, optical line terminal (OLT) cards, IP capacity and others. If all facilities are duplicated, the cost per user increases significantly. This large incremental cost hurts the interest of residential users who prefers low cost of service. Thus, while providing high protection coverage to business users, the residential users must be shielded from a high cost increase.

Paper [5] focuses on TWDM-PONs and provides a comprehensive insight into the most efficient protection schemes until the remote node 1 (cf. Fig. 1). This paper builds up from the preliminary results obtained in [5] to construct simultaneously a reliable end-to-end network for business service and a cost-effective network for residential service. We propose various resilient schemes with varying degree of protection for residential and business users. For the proposed schemes, we analyze the protection coverage, impact of failure, connection availability, and cost. From the operators' point of view, reducing the impact of a failure (i.e. to minimize the number of end users affected by a single failure) should be considered in the first place. Meanwhile, the end users (in particular business users) typically require a certain guaranteed level of connection availability in order to lower the risk of service interruption. The incremental costs of investment for protected service should be low. Furthermore, the protection times should be within the required bounds of the services. T1/E1 and plain old telephone services (POTS) require 50 ms and 120 ms protection times respectively, so for these services to be provided as protected, the network should support 50 ms protection times [6]. For an unprotected system, service restoration could take the time required to repair the failure.

The remainder of this paper is organized as follows. Section II describes different variants of TWDM-PON architectures. Section III introduces parameters and scenarios considered for the reliability assessment. Section IV presents the proposed resilient schemes. In Section V, we evaluate them in different population areas and the final section presents our conclusions.

II. TWDM-PON ARCHITECTURES

In this section, we describe different variants of TWDM-PON architectures. Typically, they have a tree topology, with the OLT as the root of the tree and the optical network units

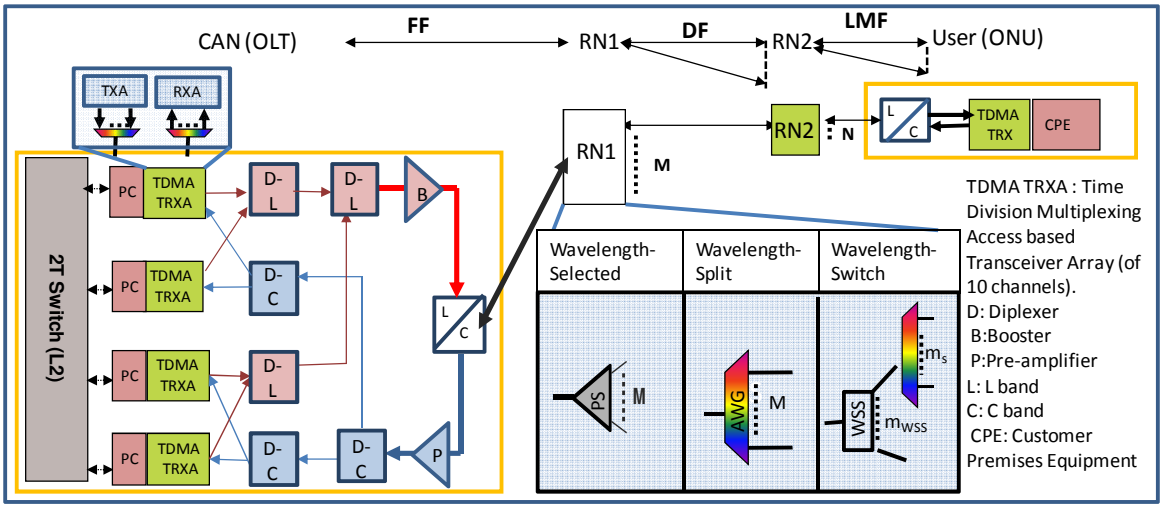

Figure 1: Basic TWDM-PON architecture

(ONUs) at the leaves (see Fig. 1). There are also some proposals for ring-based architectures. Ring based architectures can employ a fast protection switching mechanism from synchronous optical network/synchronous digital hierarchy (SONET/SDH) technology, but they require the use of add–drop nodes, which increase the insertion loss, costs, and power consumption. Moreover, a large part of the duct network in developed countries was laid before the appearance of SONET/SDH ring network topology, and thus ring solutions do not provide short-distance paths between nodes [8].

Fig. 1 shows the detailed system design of the OLT. Note that we have shown four transceivers in the figure corresponding to 40 upstream (ONU to OLT) and downstream (OLT to ONU) channels. For 80 channels configuration, we will require 8 transceivers and 15 diplexers [7]. We use photonic integrated circuits (PIC) based transceivers arrays (TRXA) and a series of L and C band diplexers to multiplex and demultiplex downstream and upstream channels respectively. In a next-generation scenario, the OLT is located at the central access node (CAN) which is connected to remote node 1 (RN1), typically at the local exchange (LE), by the feeder fiber (FF). Through the distribution fiber (DF), each output port of RN1 goes to a different remote node 2 (RN2) which includes a power splitter (PS), and then each output port of the PS is connected to a different ONU by the last mile fiber (LMF). According to the RN1 configuration, we have three variants of TWDM-PON architectures. For all variants, we have assumed 80 upstream and downstream wavelength channels. For all variants, we assume a booster (downstream) and a pre-amplifier (upstream) at the OLT and a RE at RN1.

A. *Wavelength Selected TWDM-PON*

As shown in Fig. 1, RN1 of a wavelength selected TWDM-PON consists of a PS. Consequently, this implies a broadcast and select behavior since each ONU has to select ultimately its assigned wavelength and time slot. This approach has the highest flexibility on resource allocation among all TWDM-PON variants, but at the expense of a huge insertion loss occurred by the high power splitting ratio. For this study, a 1:32 splitter has been assumed at both RN1 and RN2 (i.e. M=N=32).

B. *Wavelength Split TWDM-PON*

A wavelength split TWDM-PON uses arrayed waveguide gratings (AWG) at RN1. In this way, one dedicated wavelength is routed to each RN2. Although this configuration is limited in flexibility on wavelength allocation, it has a relatively long reach due to the low insertion loss of an AWG. We consider a 1:80 AWG at RN1 and a 1:16 splitter at RN2 (i.e. M=80, N=16).

C. *Wavelength Switched TWDM-PON*

In wavelength switched TWDM-PON, active components like wavelength selective switches (WSS) are installed at RN1. WSS provide flexibility in wavelength allocation, as wavelengths can be configured according to the load variations, like day and night. However, flexibility of bandwidth allocation over a WSS is restricted compared to a PS [3]. For this study, we consider a 1:4 WSS, and a 1:10 AWG at RN1 and a 1:32 splitter at RN2 (i.e. M=$m_{WSS} \times m_S$=40, N=32).

III. Parameters and Scenarios for Reliabilty Evaluation

In this section, we discuss the used parameters and the scenarios considered for the reliability evaluation.

A. *Parameters*

Four parameters are considered as important for the reliability measurement: protection coverage, availability, failure impact robustness and cost.

1) *Protection Coverage*

Protection coverage is a simple method to evaluate reliability. It measures the percentage of number of duplicated architectural elements (i.e. components and fibers) to the total number of architectural elements. If all elements are doubled, the network will have protection coverage of 100%.

2) *Component and Connection Availability*

Asymptotic availability is defined as the probability that a component is operable at an arbitrary point of time. The approximate equation of availability A for a certain component can be expressed as:

$$A = 1 - \frac{MTTR}{MTBF} \quad (1)$$

with: *MTTR* = mean time to repair
MTBF = mean time between failures

MTBF and MTTR values of each element are given in [2]. Connection availability means the probability that a logical connection (e.g. between the OLT and ONU) is operable.

The optimal value of the availability depends on the network operator and the customers in operation. However, we feel that an availability of > 0.9999 is sufficient for NG-PON networks as the aggregation networks are also built with an availability of 4 nines [10].

3) Failure Impact Robustness (FIR)

Besides availability, we consider another important resilience parameter, namely the failure impact robustness (FIR), which is comparable to the figure of merit (FOM) introduced in [9]. The failure of an OLT (at the CAN) impacts all customers whereas the failure of an ONU (at the user end) affects just one customer. In reality, network operators are often more worried about a single failure with large impact than many small uncorrelated failures (with the same total impact), since a single large impact failure does more harm to the company image and could lead to negative press releases. Moreover, an operator will feel more economic stresses due to failures with a large impact as it involves a high one-time penalty cost compared to failures with a small impact where the penalty cost is gradual. To reflect this reality, the FIR is a better measure. For a specific component, it is given as:

$$FIR_{component} = \frac{1}{CAF \times UnAv} \quad (2)$$

with: *CAF* = Number of customers affected by a failure
UnAv = Unavailability of the component=1-A

The FIR of the end-to-end (EtoE) connection, consisting of a sequence of components (e.g. OLT, ONU, RN1, RN2) can be evaluated by:

$$\frac{1}{FIR_{EtoE}} = \sum \frac{1}{FIR_{component\ i}} \quad (3)$$

For a robustly built network (with an availability of 0.9999), a failure in the network with FIR > 10 will affect less than 1000 users at the same time. We assume that a network should have at least a FIR > 10. A FIR of 100 means less than 100 customers are hit at the same time, which can be considered rather safe for the operators. Therefore, we believe that realistic networks should have a FIR between 10 and 100.

4) Cost of Protection

The incurred cost due to protection must be as low as possible for low cost per users. The most straightforward way of the cost calculation is to sum up the component, fiber and trenching cost incurred in protection. For better insights in techno-economic aspects of protection, we evaluate another parameter, referred as protection per unit cost, which represents the increment in network availability possible with the incremental cost. This parameter gives us an indication to figure out the most cost efficient ways to increase network availability.

B. Scenarios

We consider three scenarios for the reliability evaluation: dense urban (DU), urban (U) and rural (R). For the fiber availability, we have assumed a downtime of {0.5, 0.3 and 0.1} hr/(km-year) for DU, U and R, respectively. We make a difference between the working path (WP) and backup path (BP) required for protected configurations (see section IV). The typical fiber length of the WP and BP in the three scenarios varies and depends on the degree of node consolidation. Node consolidation is the replacement of a number of active network sites, i.e. central offices (COs), with a CAN. For our calculations, we have considered two node consolidation scenarios: High (H) and Low (L) assuming a CAN replaces 80 and 4 COs, respectively. Table 1 shows the fiber lengths for the different scenarios, as calculated in [11] for a household penetration of 100%. The fiber length of the BP will be larger than the WP because the BP fiber will be laid in a disjoint duct.

Table 1: Fiber lengths for the considered scenarios

Node Consolidation		H			L		
Scenarios		DU	U	R	DU	U	R
FF length (km)	WP	6	23	40	1	4	9.5
	BP	11	38	72	3.5	12	28
DF length (km)	WP	1	1.5	2	1	1.5	2
	BP	1	1.5	2	1	1.5	2
LMF length (km)	WP	0.5	1	1.5	0.5	1	1.5
	BP	0.5	1	1.5	0.5	1	1.5

IV. RELIABLE ARCHITECTURES

In this section, we discuss different protection options and then propose reliable architectures.

A. Protection Scenarios

The failure of an OLT impacts all customers and thus an unprotected OLT has the lowest value of FIR after the FFs, which keeps the EtoE FIR of any configuration below an acceptable threshold [5]. Therefore, it is crucial to provide protection at the CAN, where the OLT is located. There are two ways of an OLT protection: duplex and a dual-parented (or dual-homed). In the former, the working and backup FF, which connect the OLT to the first-stage split, are both terminated in the same node, while in the dual-parenting case, the working and backup OLTs are geographically separated, as shown in Fig. 2 (a). The second provides a higher level of reliability because it leads to independent power outage failures and increases the network reliability against local disasters. Moreover, the backup fiber follows a disjoint geographical route to provide maximal protection against cable cut, and thus, any cost savings because of the two OLTs at the same physical location are minimal. Dual-parented scheme needs inter-OLT signaling to control the switching for protection. The OLTs are interconnected through the aggregation network, and inter-OLT signaling between the OLTs can be done through the aggregation network. The working OLT has to signal periodically the identity, service level agreement (SLAs), and round-trip time (RTT) of the ONUs that are connected. The need of the communication of the control information is imperative to reduce the protection time. As otherwise, the backup OLT has to re-discover and re-register the ONUs and the discovery time, which is the time between a new ONU to

register and start transmitting data frames, can be as large as 10 seconds or more [12]. Thus, for protection time to be within 50 ms time interval, the backup OLT needs on beforehand the information of the registered ONUs. The primary OLT communicates this information to the backup OLT management card through the inter-communication channel. Another important distinction can be done either by duplicating the line terminal (LT) or by full OLT duplication. We refer LT as the combination of the transceivers, diplexers and the band splitter. Protecting the LT itself does not show much benefit to improve the unavailability and FIR of the OLT. It is because of the low availability of the active components such as the switch, power supplies, booster/preamplifier. Therefore, we consider full OLT duplication. Another differentiation in the protection schemes is in the way the OLTs are connected to the FFs. One is to use an extra 3dB coupler to combine the OLTs and FFs (cf. Fig. 2 (b)). The other is to connect each OLT output directly to each FF. The latter scheme does not need an additional coupler and has a higher connection availability and FIR. Besides, the first scheme will require extra fiber deployment for dual parented scenario. In this paper, we consider the dual-parented scheme with fully duplicated OLTs, which are connected, directly to the FFs.

Protection of the FF is most significant for long FF. From an operator perspective, as soon as the FF length becomes more than 1 km [5], the FF becomes the most dominant factor that influences reliability. Normally, FF protection duplicates the fiber, and as mentioned in section III, the BP FF is laid in a disjoint duct with minimal geographical overlap.

The protection of the RN1 is also significant from the FIR perspective and availability. The use of active components like WSSs (for wavelength switched TWDM-PON) and RE in RN1, increase the unavailability of the RN1 and thus it has to be protected for the business users. For the protection between the LE and the end user, the DF and LMF can also be duplicated. As this approach is too expensive for general deployment and the protection between the LE and end-users does not significantly affect the FIR, the network operators will not be in favor of protection after the LE for all users. However, end-to-end customer protection is required for business customers or services requiring high reliability such as e-health, and remote consultation of doctors.

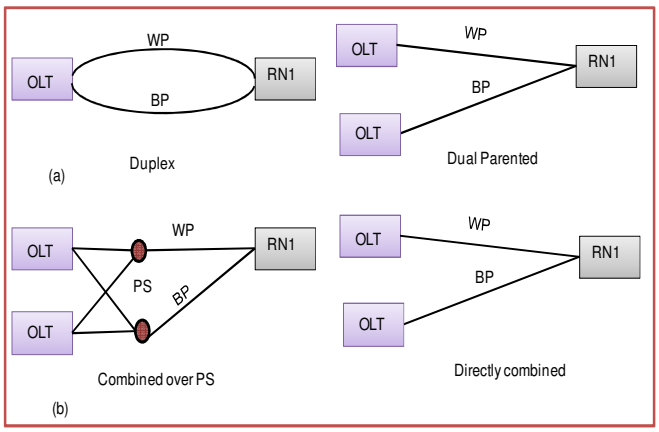

Figure 2: (a) Duplex and dual parented schemes and b) Different ways in which the OLT and feeder fiber can be combined.

B. *Protected Architecture Designs*

Based on the explanations given in section IV.A, we propose four variants of protection schemes, shown in Fig. 3. The protection schemes vary in terms of protection coverage that they offer to the business and the residential users. All schemes are with dual parenting and full OLT duplication. The FFs are coupled directly to the OLT line terminal. The inter-communication link is present between two OLTs through the aggregation network. The backup OLT can be used for 1: P protection. In the backup OLT, we can use either a fiber switch or a WSS as switch. The increase in cost per user of using WSS is insignificant as a large number of users share it. The use of WSSs provides protection against multiple OLT failures. Since, the backup capacity of an OLT is typically the same as the working OLT, not all but at least every business user can be protected. In addition, another advantage of using WSSs is to safeguard against simultaneous failures of many transceivers in multiple OLTs at the same time.

Scheme A is with only OLT and FF protection. For business users, we use an ONU in which the transceiver is duplicated to increase reliability. An ONU has a high unavailability and protecting ONUs increases the reliability of business users. Scheme B is with LMF protection for business users. A business user receives its service from two disjoint LMFs. Scheme C is with DF, LMF and PS protection for business users. Scheme D further extends the protection of scheme C with RN1 protection. Clearly, the level of reliability and the cost of protection increase from scheme A to scheme D for business users. These schemes offer an increased protection for business users, but the same level of protection for residential users.

V. ARCHITECTURAL EVALUATION

In this section, we evaluate the resilience and cost of various architectures.

1) *Protection Coverage*

Fig. 4 shows the protection coverage of the various protection schemes. We have considered seven main facilities: OLT, FF, RN1, DF, RN2, LMF, and ONU; and in protection coverage, we measure the facilities that are protected (either partially or completely). The protection coverage increases from scheme A to D for business users. In scheme D, all facilities are protected for business users, and thus it provides 100% coverage. Furthermore, scheme A provides 43% coverage (with OLT, FF, and ONU protection); scheme B provides 57% coverage (with OLT, FF, LMF and ONU protection); and scheme C provides 86% coverage (with OLT, FF, DF, PS, LMF and ONU protection). For residential users, the protection schemes provide about 29% protection coverage with only OLT and FF protection.

2) *Availability*

Fig. 5 shows the component availability (without fibers) of business and residential users of various TWDM-PON flavors when different protection schemes are applied. Generally, the unprotected and protection schemes achieve a high reliability for wavelength selected and wavelength split and minimum reliability for wavelength switched TWDM-PON. However, the availability of business users of various architectures in

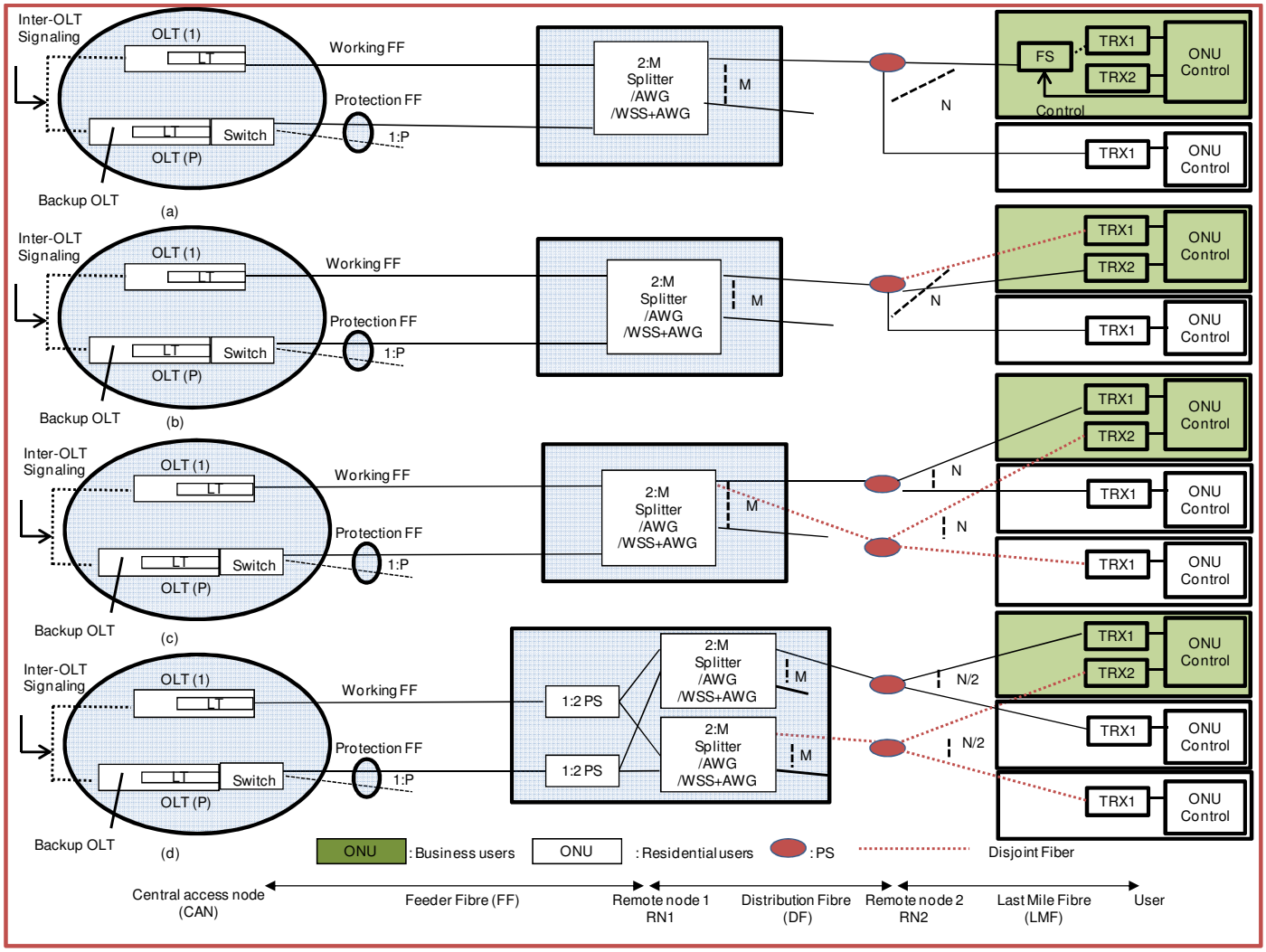

Figure 3: Reliable architectures with a varying degree of protection. Four schemes are proposed A, B, C and D.

scheme D does not vary significantly because RN1 is fully protected weeding out any drop in reliability that stems from using active components or less reliable passive components (like AWG instead of PS). Fig. 6 shows the availability of wavelength switched TWDM-PON in various populated scenarios like dense urban, urban and rural. The wavelength switched TWDM-PON is used as an example instead of showing all possible combinations of results. In addition, the effect of different scenarios will be the same for all TWDM-PON variants. Note that the different scenarios have different lengths of working and protected FF, DF and LMF (cf. Table 1). The availability is computed using the fiber availability in different scenarios and using the component availability shown in Fig. 5. Fig. 6 shows that, for full end-to-end protection for business users (scheme D), we achieve an availability of close to five 9s and the availability is fairly independent of the link lengths. All protection schemes have minimum reliability in urban scenarios. The unavailability depends upon the fiber failure rates and the fiber lengths. The urban scenario has a higher fiber cut probability than the rural scenario while it has longer fiber lengths than the dense urban scenario. The combination of these two parameters maximally reduces the fiber availability in the urban scenario.

3) Failure Impact Robustness (FIR)

Fig. 7 and 8 show the FIR performance. First, we note that the FIR performance is for the network and is inconsequential to the users. The FIR performance of various TWDM-PON flavors is synonymous to the availability. FIR is minimal for wavelength switched, medium for wavelength split and best for wavelength selected. Furthermore, again wavelength switched TWDM-PON is used as an example to show the effect of different scenarios on FIR. Fig. 8 shows that the urban scenario has minimum FIR.

4) Cost

In accordance with the availability and FIR analysis, we first give the impact of various protection schemes on the cost for various flavors of TWDM-PON in Fig. 9. The cost calculation methodology and numbers are from [7]. Fig. 10 gives the cost evaluation of wavelength switched TWDM-PON in all scenarios. The fiber cost is assumed as two-Euro cents

per meter. The cost of the solution increases from dense urban to rural because of increased fiber lengths. There is even an increase in the cost for residential users in scheme D, as there are a lower number of users per DF. The cost of full protection for business users increases between 180 and 215 EUR respectively, and the cost of protection for residential users increases between 30 and 40 EUR respectively, depending upon the scenario. However, this cost does not include trenching. We evaluate the trenching cost in various proposed schemes in various scenarios in Fig. 11. The trenching cost is assumed as 40, 35 and 30 EUR per meter for the dense urban, urban and rural scenario respectively. The trenching cost depends linearly on the amount of new trenching needed for protection. If trenching is required for 100% new fiber deployment, then the impact of the increased cost per user will be very high (more than 50 kEUR) and thus it can be a showstopper. Further, if a low trenching fraction is required, then scheme C has similar cost implications as scheme B while it offers a better protection coverage. Similarly, at a very high trenching fraction, the cost implications of scheme C and scheme D are tantamount, and scheme D should be chosen. Thus, the final choice between the schemes will depend on the trenching fraction, which is dependent on many factors like the degree of node consolidation, the population scenario, and the fiber deployment routes. A more complex and detailed evaluation of the trenching fraction and its dependence on the scenario can be studied assuming analytical or geographical models for the trenching length [13], [14].

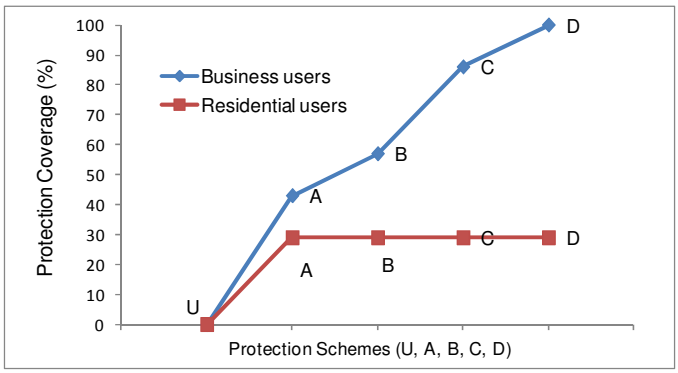

Figure 4: Protection coverage in unprotected (U) and protection schemes (A, B, C and D) of business and residential users.

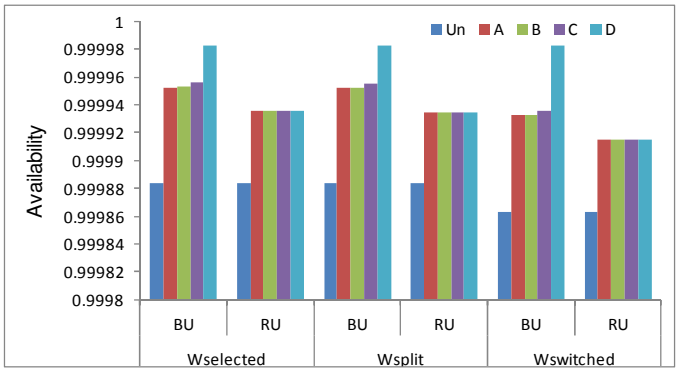

Figure 5: Availability in unprotected (U) and protection schemes (A, B, C and D) of business and residential users of various TWDM-PON flavors.

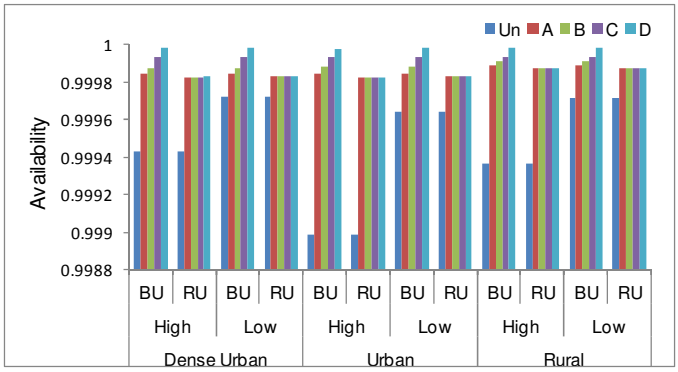

Figure 6: Availability in unprotected (U) and protection schemes (A, B, C and D) of business and residential users of wavelength switched TWDM-PON in dense urban, urban and rural scenarios.

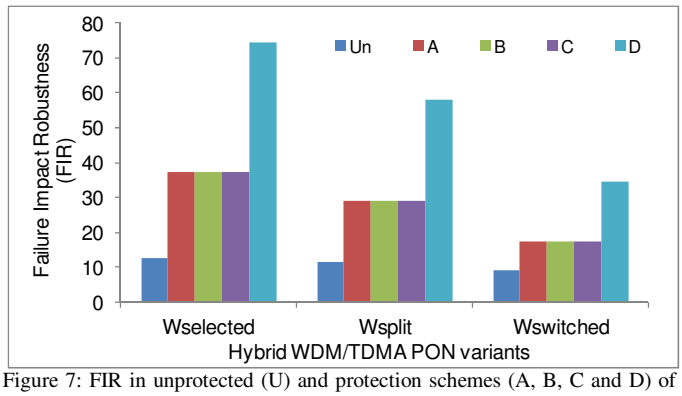

Figure 7: FIR in unprotected (U) and protection schemes (A, B, C and D) of business and residential users of various TWDM-PON flavors.

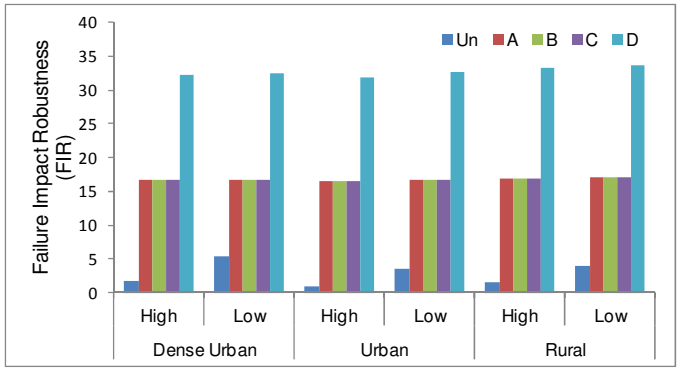

Figure 8: FIR in unprotected (U) and protection schemes (A, B, C and D) of business and residential users of wavelength switched TWDM-PON in dense urban, urban and rural scenarios.

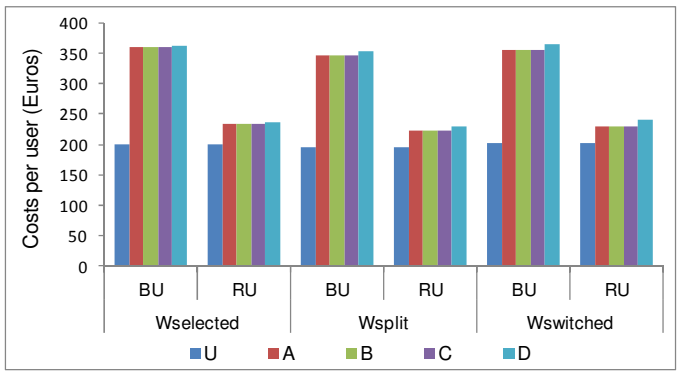

Figure 9: Cost in unprotected (U) and protection schemes (A, B, C and D) of business and residential users of various TWDM-PON flavors.

Another useful parameter that is investigated is protection per unit cost. One of the main reasons for protection is to avoid penalties due to loss of services that an operator has to pay to business and residential users. The penalty will be proportional to the unavailability of the network. The penalty can be minimized by increasing the availability of the network, which can be increased by improving various components' availability or fiber protection. Fig. 12 shows the incremental protection per unit cost while protecting various systems. For fiber, parameters of the urban scenario are assumed. The figure shows that the availability can be increased most cost effectively by increasing FF or OLT protection. This is clearly due to the fact that the OLT and FF are single units and the improvement in their availability impacts the whole network, whereas to improve the availability of the network by

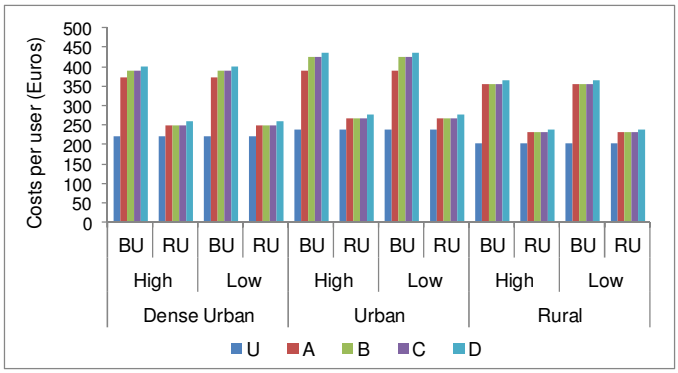

Figure 10: Component and fiber cost in unprotected (U) and protection schemes (A, B, C and D) of business and residential users of wavelength switched TWDM-PON in dense urban, urban and rural scenarios.

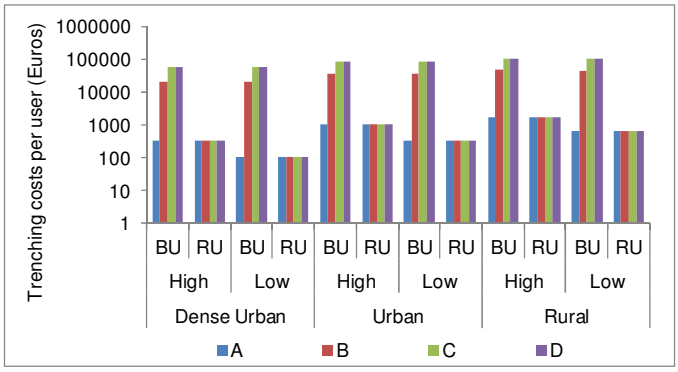

Figure 11: Trenching cost in various protection schemes (A, B, C and D) for business and residential users in dense urban, urban and rural scenarios.

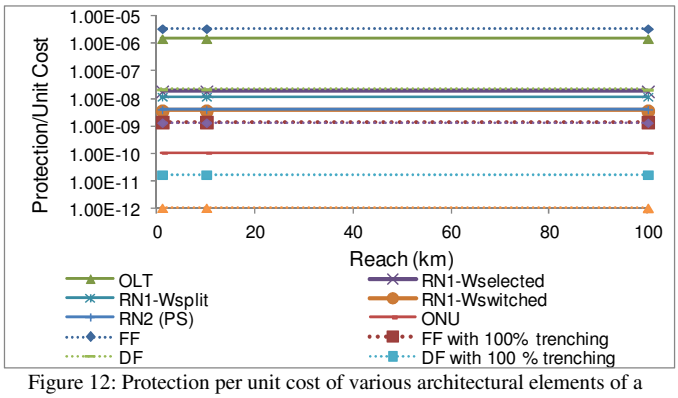

Figure 12: Protection per unit cost of various architectural elements of a TWDM-PON.

increasing the reliability of the ONUs, 1000 or more ONU boxes have to be upgraded. Fig. 12 demonstrates some of the cost efficient ways to improve availability.

VI. Conclusions

In this paper, we propose four different protection schemes to foster end-to-end reliability for business users, and central access node and feeder fiber protection for residential users. The proposed schemes are analyzed for protection coverage availability, failure impact robustness and cost, in different populated scenarios. The dual parented scheme with full OLT duplication is the most efficient reliable solution, which can be further augmented with full remote nodes and optical distribution network (ODN) duplication for business users. There is an incremental protection cost of between 180 and 215 EUR for business users, and 30 and 40 EUR for residential users. The trenching cost is the main deciding factor in protecting the ODN and can be a showstopper if 100% new trenching is required. OLT and feeder fiber protection is found to be the most cost efficient way to increase network reliability while decreasing odds of large customer hit outs.

Acknowledgment

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 249025 (ICT-OASE).

References

[1] G. Kramer, M. De Andrade, R. Roy, and P. Chowdhury, "Evolution of optical access networks: architectures and capacity upgrades," *Proceedings of the IEEE*, vol. 100, pp. 1188 – 1196, May 2012.

[2] OASE Project, D4.2.1: Technical assessment and comparison of next-generation optical access system concepts, Oct. 2011.

[3] A. Dixit et al., "Flexibility evaluation of Hybrid WDM/TDM PONs", *IEEE ANTS 2011*, Bangalore, India, Dec. 2011.

[4] Business class services over a GPON Network, available at: http://www.fujitsu.com/downloads/TEL/fnc/whitepapers/BusinessClass-GPON.pdf

[5] A. Dixit et al., "Efficient Protection Schemes for Hybrid WDM/TDM Passive Optical Networks," *Workshop on New Trends in Optical Networks Survivability, IEEE ICC*, Ottawa, Canada, June 2012.

[6] ITU-T Rec. Series G.984.1, Mar. 2008.

[7] A. Dixit, B. Lannoo, D. Colle, M. Pickavet, and P. Demeester, "Wavelength Switched Hybrid TDMA/WDM (TWDM) PON: a Flexible Next-Generation Optical Access Solution [Invited]," *ICTON*, Coventry, U.K, July 2012.

[8] M. Ruffini et al., "Deployment strategies for protected long-reach PON," *J. Opt. Commun. Netw.*, vol. 4, pp. 118-129, Feb. 2012.

[9] J. Kim, S. Yen, S. Fu, and L. G. Kazovsky, "Resilient optical access networks: optimization on the number of spikes in the StarRing", *Workshop on Photonic Technologies for Access and Bio-Photonics*, Jan. 2011.

[10] M. Vogt, R. Martens, and T. Andvaag, "Availability modeling of services in IP networks", *DRCN*, Banff, Canada, Oct. 2003.

[11] OASE Project, D5.1: Overview of methods and tools, Sep. 2010.

[12] ITU-T Rec. Series G.984.1, Mar. 2008.

[13] B. Lannoo et al., "Techno-economic feasibility study of different WDM/TDM PON architectures," *ICTON,* Munich, Germany, June-July 2010.

[14] A. Mitcsenkov et al., "Geographic Model for Cost Estimation of FTTH Deployment: Overcoming Inaccuracy in Uneven-populated Areas," *ACP*, Shanghai, China, Dec. 2010.